REMARKS

This paper is in response to the Final Official Action mailed April 2, 2008 and the Advisory Action mailed on June 9, 2008. This paper accompanies a Request for Continued Examination (RCE) under 37 C.F.R. § 1.114. In the present paper, Claims 1, 11, 13, 14, 19 and 21-26 are amended, claims 34 and 35 are added and claims 4, 5, 15, 16, 28 and 29 are canceled. Claims 8, 20 and 32 were canceled in a previous paper. Claims 1-3, 6, 7, 9-14, 17-19, 21-27, 30, 31 and 33-35 are now presented for the Examiner's consideration in view of the following remarks.

Present Application

The inventors have discovered a system and method for identifying and communicating with potential clinical trial participants. The invention addresses two long-standing interrelated problems. First, the problem of data anonymity has, in the past, restricted systems for identifying potential clinical trial participants to systems that work on a small, localized scale (present specification at [0004]-[0005]). Second, there is a need to reliably identify a large pool of potential clinical trial participants from which to choose, due to the often narrow participant selection criteria of a given trial, and the high cost of replacing an incorrectly selected participant (present specification at [0003]-[0004]).

The inventors have solved the problem of data anonymity by replacing the identities of patients in a database with *encrypted versions of the identities*. To the inventors' knowledge, that advance is unique in the field of clinical trial candidate selection. The inventors have furthermore utilized a database containing transactions between health care providers and payers to identify clinical trial candidates. Using such a database has significant advantages in candidate pool size and data quality. To the inventors' knowledge, however, such a database had never been utilized to identify clinical trial candidates, at least in part because of patient anonymity concerns. The present invention solves both longstanding problems.

In the Final Official Action, the Examiner has rejected claims 1-6, 9-19, 21, 23-30 and 33 under 35 U.S.C. § 103(a) as unpatentable over U.S. Patent Publication No. 2002/0099570 to Knight ("Knight") in view of U.S. Patent Publication No. 2004/0078238 to Thomas et al. ("Thomas") and further in view of U.S. Patent No. 6,915,266 to Saeed et al. ("Saeed"); has rejected claims 7 and 31 under 35 U.S.C. § 103(a) as unpatentable over Knight in view of Thomas, further in view of Saeed and further in view of U.S. Patent Publication No. 2003/0208378 to Thangaraj et al. ("Thangaraj"); has rejected claim 22 under 35 U.S.C. § 103(a) as unpatentable over Knight in view of Thomas, further in view of Saeed and further in view of U.S. Patent No. 5,111,395 to Smith et al. ("Smith").

Claim Amendments

Each of the independent claims in the present case has been amended to require the *encryption* of patient identities. For example, claim 1 now includes the additional step of:

> encrypting the identities of the patients to create encrypted versions of the patient identities.

Those encrypted versions of the identities are then used to replace the unencrypted versions in the patient data, and the patient data is forwarded to a clinical trial candidate identification service. Support for those amendments may be found in the present specification at least at paragraphs [0046]-[0050].

Claim 4, which required encrypting the identities of the patients to create secure patient codes, has been canceled because the present amendment incorporates similar limitations into independent claim 1. Claim 5, which claimed an alternative embodiment including unique identification codes used with a look-up table, has been canceled as a different embodiment from amended claim 1. Claim 11 was amended for consistency with claim 1.

The other independent claims, together with their dependent claims, have been amended in a corresponding manner.

By substituting encrypted versions of the patient identities into the patient data, that information can be retrieved from the patient data without the need to consult a look-up table. A version of the actual information is contained in the patient data itself. There is therefore no need to store a look-up table at the Data Exchange Service.

As noted, limitations similar to those of canceled claim 4 were incorporated into the independent claims. Claim 4 was rejected in the Final Official Action as obvious over Knight in view of Thomas and further in view of Saeed. Specifically, the Examiner identified Thomas as teaching "replacing the identities of the patients in the patient data with secure patient codes comprises encrypting the identities to create patient codes." The Examiner points to passages in Thomas disclosing the use of "anonymous identifiers" together with a stored table pairing the identifiers with actual data.

The cited passage describes FIG. 2 of Thomas. FIG. 2 shows the generation of the anonymized "assigned patient ID" by incrementing the previous ID by 1 (Thomas, FIG. 2, step 58). The assigned patient ID is substituted in the data header (step 62) and paired with the actual ID information in a stored table 44 called "pair_list.txt" (step 60). In other words, Thomas uses an identifier together with a look-up table.

The patient identity in Thomas is not encrypted, and no "encrypted version" of the patient identity is used to replace the original patient identity, as required by the amended claims. Instead, Thomas uses an identifier in conjunction with a stored look-up table to anonymize the data. Because neither Thomas nor any other art of record teaches encrypting the patient identity and replacing the patient identity with an encrypted version of the patient identity, Applicants assert that independent claim 1, together with those claims depending from claim 1, are patentable. Applicants further assert that independent claims 13, 23 and 24, which contain corresponding limitations, together with their dependent claims, are patentable for the same reasons.

New Claims

Claims 34 and 35, which depend from claims 1 and 24, respectively, have been added. Those new claims require that the claims encryption of the patient identities comprise a one-way hash of that data. The new claims are fully supported in the specification at least at [0041]. Applicants assert that no art of record discloses performing a one-way hash of the patient identities and contact information. For that additional reason, Applicants submit that claims 34 and 35 are patentable.

Response to Examiner's Advisory Action

The Examiner has found the Applicants' Remarks in the Request for Reconsideration to be unpersuasive. Applicants respectfully traverse that finding. Specifically, in response to what the Examiner has identified as Applicants' argument (1), the Examiner states that the motivation for combining Knight and Thomas is found in Thomas' statement that "in order to properly support research and development . . . data will often need to be shared between hospitals and research and design facilities both internal and external to a given hospital," and that "in order to share that data, the patient's confidentiality needs to be protected" (Advisory Action at 2). Applicants assert that the broad statement in Thomas to "support research and development" is not a suggestion to apply Thomas' anonymizing tool to identify clinical trial candidates. Thomas is instead clearly referring to the sharing of clinical data in actual research, not candidate selection. The identification of trial candidates is a different problem from conducting research. For example, in clinical trial candidate selection, the candidates and their doctors must be contacted and the flow of confidential information is therefore different from that involved in conducting research. Applicants therefore reassert that there is no motivation to combine Knight with Thomas.

As to the argument identified by the Examiner as Applicants' argument (2), the Examiner states, "The Examiner is using the Saeed et al. reference to show that it is well known in the art to receive a clinical data record from an entity controlling a database containing transactions between health care providers and payers" (Advisory Action at 2). Applicants assert that the claims, in addition to requiring *receiving* clinical data from a source containing transactions between health care providers and payers, require numerous additional operations to be performed on that same data. Those additional operations (e.g., encrypting, forwarding, decrypting) permit the use of that data in *identifying clinical trial candidates*. Applicants are aware of no prior use of health care transactions data for that purpose. The Examiner has pointed to no reference teaching that advance, and has identified no motivation to use Saeed's teachings for that purpose. Applicants therefore reassert that there is no motivation to combine Knight and Thomas with Saeed.

Applicants therefore assert that each of the currently presented claims is patentable for those additional reasons.

Conclusion

Applicants therefore respectfully assert that claims 1-3, 6, 7, 9-14, 17-19, 21-27, 30, 31 and 33-35 and are in condition for allowance, and earnestly request that the Examiner issue a Notice of Allowance.

Should the Examiner have any questions regarding the present case, the Examiner should not hesitate in contacting the undersigned at the number provided below.

Respectfully,

By Donald B. Paschburg
Donald B Paschburg
Reg. No. 33,753
Telephone: 732-321-3191

Siemens Corporation
Intellectual Property Department
170 Wood Avenue South
Iselin, NJ 08830

Date: 8/4/2008